



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/088,541	03/19/2002	Gary S Simpson	124-928	6928

23117 7590 05/11/2006

NIXON & VANDERHYE, PC  
901 NORTH GLEBE ROAD, 11TH FLOOR  
ARLINGTON, VA 22203

EXAMINER
----------

BLUDAU, BRANDON S

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/088,541	<b>Applicant(s)</b> SIMPSON ET AL.	
	<b>Examiner</b> Brandon S. Bludau	<b>Art Unit</b> 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication:
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 12 January 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-43 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-43 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This office action is in response to amendments filed on December 22, 2005 and January 12, 2006. Claims 1-37 have been amended and claims 38-43 have been added. Therefore claims 1 - 43 are pending.
2. The Examiner acknowledges and appreciates the Applicant's making aware the Examiner's failure to indicate acknowledgement of foreign priority. This acknowledgment may be noticed on the corresponding PTOL-326.
3. The Examiner rescinds the objection to the specification regarding the Abstract as the previous Abstract was discovered in the papers filed March 19, 2002 and further this point is moot in view of the newly submitted Abstract.
4. The Examiner acknowledges the amendments to claims 19-31 and consequently withdraws the 101 rejection made previously, regarding non-statutory subject matter as the amendments place the claims in direction to statutory subject matter.
5. The Examiner acknowledges the amendment to claim 13 and consequently withdraws the 112 rejection as the changes made overcome the indefinite claim language. Furthermore the Examiner clarifies the previous position in that claim 11, which claim 13 directly depended upon, recites: "a database computer system"; this necessarily is a single system thus claim 13 was indefinite as it was directed to "a plurality of database computer systems".

### ***Response to Arguments***

6. Applicant's arguments filed on 22 December 2005 and 12 January 2006 regarding the use of Baker as directed towards "requestable datasets" in claims 1, 19

Art Unit: 2132

and 32 have been fully considered but they are not persuasive. The Examiner notes that the requestable datasets are represented by the URLs. The URL serves as an address to particular data, and as the URLs are grouped in sets, the data they address make up the requestable datasets. The datasets are requestable by using the URLs (see column 4 lines 6-15).

7. Applicant's arguments filed on 22 December 2005 regarding the use of Baker as directed towards "associating each dataset with a dataset access category" in claims 1, 19 and 32 have been fully considered but they are not persuasive. The Examiner notes that the IDs as cited are clarified in the text in column 4 lines 47-49 as also previously cited. Furthermore greater clarification is offered in column 4 lines 53-56 wherein the identified class which may contain user or terminal IDs may be widely understood to represent an access category.

8. Applicant's arguments filed on 22 December 2005 regarding the use of Baker as directed towards granting access to "user group members associated with an appropriate data access category" in claims 1, 19 and 32 have been fully considered but they are not persuasive. As discussed above, the users may be grouped in classes as cited in column 4 lines 47-56.

9. Applicant's arguments filed on 22 December 2005 regarding the use of Baker and Davis to disclose wherein "the computer-based identifying means is an X.509 certificate" in claim 4 have been fully considered but they are moot in view of the clarifications made regarding Baker as discussed in claim 1. The Examiner notes that Baker does disclose the limitations of claim 1, thus the rejection is maintained.

10. The Examiner acknowledges the argument pertaining to the use of Edd pertaining to claim 6 and thanks the Applicant for pointing out the mistaken use of this reference. New grounds of rejection have been cited below.

11. The Examiner acknowledges the argument pertaining to the use of Baker in view of Davis in view of Harn and asserts that these arguments are moot based on new grounds of rejection.

12. The Examiner acknowledges the argument pertaining to claim 10, but these arguments are moot due to the subsequent clarification of Claim 1, which claim 10 depends upon.

13. The Examiner acknowledges the arguments pertaining to claims 14-16 regarding the use of Hayman, but these arguments are moot in view of the further clarification of claim 1, which claims 14-16 depend on.

14. The Examiner acknowledges the arguments pertaining to claim 18, but they are moot in view of the clarification to claim 1.

15. The Examiner acknowledges the arguments to claims 22, 24-30, 33-37, but they are moot due to the further clarification of the independent claims.

#### ***Claim Objections***

16. Claims 2 and 20 are objected to because of the following informalities: line 3 reads "category incorporates a or as the case may be each lower ..." The Examiner asserts that commas are appropriate within this clause after "or" and after "be".

Appropriate correction is required.

Art Unit: 2132

17. Claim 8 is objected to because of the following informalities: line 5, there should be a comma after the word "means", to read "group identifying means, and the dataset access step includes". Appropriate correction is required.

18. Claim 13 is objected to because of the following informalities: line 2, there should be a comma after "data request". Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

19. Claims 1-3, 5, 11-13, 17, 19-21, 23,29,31,32,38, 41 are rejected under 35 U.S.C. 102(b) as being anticipated by Baker (US Patent 5695898).

20. As per claim 1, Baker discloses a method for computer security to control access to data held on a computer system (columns 2,3 lines 66-3) as requestable datasets (see arguments above), said method comprising the steps of:

Allocating computer system users between a plurality of user groups, each user group corresponding to a respective data access category selected from a plurality of such categories (column 5 lines 37-43);

Associating each dataset with a dataset access category (column 4 lines 47-49 and 53-56); and

Giving access to each dataset only to user group members associated with an appropriate data access category for that dataset (column 4 lines 36-46).

21. As per claim 2, Baker discloses a method according to Claim 1, wherein user groups and data access categories have hierarchical levels in which a higher data access category incorporates a or, as the case may be, each lower data access

Art Unit: 2132

category, and the method includes allowing access to datasets by members of user groups associated with the data access category levels equal to and higher than those to which such datasets correspond (column 5 lines 6-12).

22. As per claim 3, Baker discloses a method according to Claim 1, wherein each user is associated with a computer based identifying means and the method includes the step of determining a user's identity from the identifying means (column 3 lines 54-56 and column 4 lines 36-39).

23. As per claim 5, Baker discloses a method according to Claim 1, wherein datasets are web pages and the method includes the step of gaining access to the computer network via the Internet or the World-Wide-Web (column 2 line 3 – column 3 line 8).

24. As per claim 11, Baker discloses the data maintained on at least one database computer system (World Wide Web), and dataset access is given by access control software operated on a separate access control computer system (see Fig.1 block 112) and a user gains access to data by means of access request software running on a user computer system separate from the database and access control computer systems (see Fig. 1 blocks 107-109).

Baker does not explicitly state that the access control or the access request methods are on software, but one skilled in the art would clearly see that without explicitly saying software, the method that Baker discloses and implements must be run on and therefore inherently includes software at the user, access control, and database systems.

Art Unit: 2132

25. As per claim 12, Baker discloses a firewall at the access control system (see Fig. 1 block 113).

26. As per claim 13, Baker discloses the data is maintained on a plurality of database computer systems and in response to a data request, access control software determines whether or not corresponding data access is appropriate after relaying the request to a dataset computer system having such data (column 4 lines 7-15).

27. As per claim 17, Baker characterizes the step of giving access to a dataset includes unencrypted transfer of data from datasets to which access is granted (column 5 line 45; it is known to one of ordinary skill in the art that the http protocol includes unencrypted pages).

28. Claim 19 is rejected for disclosing the same subject matter as claim 1. One of ordinary skill in the art can clearly see that the method disclosed would inherently include a computer program so that it could be implemented.

29. Claim 20 is rejected for disclosing the same subject matter as claim 2.

30. Claim 21 is rejected for disclosing the same subject matter as claim 3.

31. Claim 23 is rejected for disclosing the same subject matter as claim 5.

32. Claim 29 is rejected for disclosing the same subject matter as claim 12.

33. Claim 31 is rejected for disclosing the same subject matter as claim 17.

34. Claim 32 is rejected for disclosing the same subject matter as claim 1, wherein the network access controller is found in Baker (Fig 1 number 112).

35. As per claim 38, Baker discloses a method for controlling user access to data held on a computer system as requestable datasets, the method including:



Art Unit: 2132

Labeling the datasets with dataset access labels defining a hierarchy of data access levels,

Allocating computer system users between a plurality of user groups,

Labeling user groups with data access levels selected from a plurality of such levels; and

Giving access to a requested dataset to a requesting member of a user group labeled with a data access level which in the hierarchy is equal to or above the data access level of the requesting dataset (see claims 1 and 2).

36. Claim 41 is rejected because it discloses the same subject matter as claim 38.

***Claim Rejections - 35 USC § 103***

37. Claims 4 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claim 3 above, and further in view of Davis et al. "An Implementation of MLS on a Network of Workstations Using X.500/509".

Baker discloses all of the features of Claim 3, but does not disclose the use of X.509 certificates as the computer based identifying means.

Davis discloses using a X.509 certificate as an authentication means for use in a conditional network access architecture on page 553 under heading B. titled: *Access Server Model*.

Davis is analogous art because it discusses a computer security system very similar to Baker.

It would have been obvious at the time of the invention for one of ordinary skill in the art to modify Baker to include the use of X.509 certificates to identify the system users especially since Baker discusses using a tree structure format with directory and subdirectory listings and X.509 is the authentication framework for X.500 standard directories.

Motivation for one of ordinary skill in the art at the time of the invention to modify Baker as discussed above would have been to "provide a framework of authentication services by the directory to its users" (Davis, page 548 under heading B). It can be understood by one of ordinary skill that the Baker architecture when developed in the directory structure would clearly necessitate an enhanced form of security offered by the X.509 protocol.

Therefore, it would have been obvious to modify Baker to include X.509 certificates in order to provide authentication services to its users in the directory embodiment.

38. Claim 22 is rejected for disclosing the same subject matter as claim 4.

39. Claim 6,24,39 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claim 3 above, and further in view of Hsiao et al. (US Patent 6496944).

40. As per claim 6, Baker discloses that the datasets are web pages, but does not disclose that the step of associating each dataset with a dataset access category comprises inserting meta tags in html web page code.

Hsiao discloses wherein meta data of a database entry comprises dataset access categories (column 5 lines 39 –42 wherein the security attributes and the access control list serve as the associating access information). Hsiao is directed to a method of assisting database system restore, which the Examiner acknowledges is not analogous art. However, the Examiner notes that it is well known and practiced in the art to associate meta data with tags on documents to be stored in a database system. Typically the meta data for documents contains information about the size, type, author, summary etc. Hsiao discloses that the meta data for documents can also include security parameters and access control lists. It would also be obvious for one of ordinary skill in the art to see the parallels with meta tags on documents directed to access control in a database system and html meta tags to control access to pages on the Internet, thus making the argument analogous.

Motivation for one of ordinary skill in the art to modify Baker to include associating the dataset access categories with meta tags in html web page code, would be the same as is used in the database systems wherein it is more efficient and practical to identify an access category in the meta data of each entity, than to place all entities in category lists as would be well known by one of ordinary skill and as is practiced prevalently in the art.

41. Claim 24 is rejected because it is directed to the same subject matter as claim 6.

42. As per claim 39, Baker discloses a method according to claim 38 wherein the datasets are web pages with data access levels, and a proxy server is used to:

Receive requests for web pages from members of user groups,

Check user group data access levels against a prearranged access control list, and

Deny members of a user group access to requested web pages if they lack a data access level appearing on the access control list (column 3 lines 8-15).

Baker does not disclose wherein the labels are meta tags.

Hsiao discloses the use of meta tags as described above in the rejection for claim 6. The same argument holds for the rejection of claim 24.

43. Claim 42 is rejected because it discloses the same subject matter as claim 39.

44. Claims 7 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker. Baker discloses the method of claim 1, but does not disclose the method further including the step of performing a challenge-response exchange regarding user identification before the step of giving access to a dataset.

Baker uses a password authentication scheme to identify a user, and it is well known and practiced in the art to use challenge-response schemes in place of password login to identify users.

Therefore it would be obvious for one of ordinary skill in the art to modify Baker to use a challenge-response identification scheme instead of the password scheme.

Motivation for one to modify Baker would be to enhance the security of the identification step as would be understood by one of ordinary skill in the art. Most challenge-response methods use some sort of token or key to generate a unique response to a challenge, thus precluding one from having their credentials intercepted

Art Unit: 2132

over the network and preventing a re-use attack on the system as is common with passwords and obviating the need for a user to remember secure passwords.

45. Claim 25 is rejected for disclosing the same subject matter as claim 7.

46. Claims 8,9, 26 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker and further in view of Harn "ID-Based Cryptographic Schemes for User Identification, Digital Signature, and Key Distribution".

47. As per Claim 8, Baker discloses a method according to Claim 1 in which a user employs a user computer system to gain access to datasets to which access is controlled by an access control computer system, but does not disclose wherein that computer system has a public key for verifying signed data, wherein each user computer system incorporates a private key for signing data and user group identifying means, and the dataset access step includes:

Using the private key to sign test data provided by the access control computer system and forwarding the signed data and identifying means to the access control computer system; and

Using the access control computer system to verify the identifying means, verify the user by using the public key to verify the signed data, and determine user group and associated data access category from the identifying means.

Harn discloses a scheme, wherein "user identification can be achieved directly through a challenge-response type procedure." The steps of the scheme include using a private key to sign test data (wherein the data is a randomly selected odd number) provided by the access control computer system and forwarding the signed data and

identifying means to the access control computer system; and using the access control computer system to verify the identifying means, verify the user by using the public key to verify the signed data, and determine user group and associated data access category from the identifying means (page 758). It would be obvious for one of ordinary skill in the art to see that the user group and data access category information, while not explicitly stated, could be included in the identification data.

Harn is analogous art to Baker, as it pertains to authentication and identification schemes for identification in a network system.

It would have been obvious at the time of the invention to modify Baker to include a more robust identification scheme using the public key authentication method, as public key cryptography is a widely known and used method of authenticating users to computer systems.

Motivation for one of ordinary skill in the art at the time of the invention to modify Baker as discussed above would be to "provide user identification and digital signature" and to establish a secure and secret communication session as taught in Harn (page 757) and as would be understood by one of ordinary skill in the art.

48. As per claim 9, Baker and Harn disclose claim 8 as discussed above, wherein Harn discloses the test data is random data (page 758).

49. Claim 26 is rejected for disclosing the same subject matter as claim 8.

50. Claim 27 is rejected for disclosing the same subject matter as claim 9.

Art Unit: 2132

51. Claims 10,28,34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claim 1 above, in view of Davis, and further in view of McNabb (US Patent 6,289,462).

Baker discloses the method of claim 1 while Davis discloses providing database access to a first kind of user having a user certificate for identification purposes.

Neither Baker nor Davis discloses granting database access to a second kind of user lacking a user certificate.

McNabb discloses allowing database access to unauthorized users as anonymous access (column 18 lines 5-7 lines and column 22 lines 44-46). While McNabb doesn't explicitly describe an authentication method using certificates, one of ordinary skill in the art could easily see that the authorization method in McNabb could be performed with user certificates.

It would have been obvious for one of ordinary skill in the art to modify Baker and Davis to include a step of authentication to a user lacking a user certificate.

McNabb is analogous art because it relates to a security method that grants access privileges based on security-level attributes, with a similar access control structure as discussed in Baker.

Motivation for one of ordinary skill in the art to modify Baker/Davis to include access for users without certificates would be to allow access to public or non-sensitive data held on the database as implied in McNabb.

52. Claim 28 is rejected for disclosing the same subject matter as claim 10.

53. Claim 34 is rejected for disclosing the same subject matter as claim 10.

54. Claims 14-16, 30 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claim 1, and further in view of Hayman (US Patent 5,859,966).

55. As per claim 14, Baker discloses the method of claim 1, but does not disclose that the data access categories and the user groups and datasets with which they are associated are assigned numerical values.

Hayman does disclose that numerical values are assigned to the data access categories and the user groups and datasets with which they are assigned (column 8 line 16-18) and inherently explains the step of giving dataset access involves comparing user group and dataset numerical values to determine whether or not access is to be granted or denied. It is not an object of Hayman's invention to assign numerical numbers, but Hayman references mandatory access protocol (MAC) as described in the specification of the applicant wherein the MAC labels are stored as numeric values.

It would be obvious for one of ordinary skill in the art to modify Baker to include assigning numerical values to access categories.

Motivation for one of ordinary skill in the art to modify Baker as discussed above would have been to simplify the categorization of data objects by assigning them access numbers instead of having to arrange access lists as could be easily deduced by one of ordinary skill in the art.

56. As per claim 15, Hayman discloses that the data access categories have different sections each with a section numerical value and the step of comparing numerical values comprises comparing section numerical values of corresponding



Art Unit: 2132

sections of user group and dataset numerical values (column 8 line 16-18 wherein the sections are referred to as categorical components).

57. As per claim 16, Hayman discloses that access to a dataset is provided only if all section comparisons are satisfied (column 8 39-45).

58. Claim 30 is rejected for disclosing the same subject matter as claim 14.

59. Claim 33 is rejected for disclosing the same subject matter as claim 14.

60. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker/Hayman as applied to claim 16 and further in view of Netscape (Netscape Messaging Server Version 3.0 Administrator's Guide, Netscape Communications Corporation, 1995 pages 57-58).

Baker and Hayman disclose the method according to claim 16 as discussed above.

Baker and Hayman do not disclose the step of running checking/blocking software on the user computer system to screen incoming data for encryption to block unwanted data content.

The Administrator's Guide discloses an SSL package that allows the user to configure a specific port to block encrypted data.

The Administrator's Guide is analogous art because it relates to how data is handled over a network and Baker discloses a network that as typically found in the art supports SSL for secure data transfer. Therefore it would have been obvious for one of ordinary skill in the art to modify Baker to include the blocking software, as this is a well-known feature in data networks.

Motivation for one of ordinary skill in the art at the time of the invention to modify Baker-Hayman to include blocking software would be to allow the user the ability to specify the level of encryption for receiving and managing data as taught in Netscape page 57.

61. Claim 35 is rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claim 19 and 32 above, and Davis as applied to claim 4. Wherein the computer network for database access is that which is shown in Baker, Fig.1.

62. Claim 36 is rejected for disclosing the same subject matter as claim 6.

63. Claim 37 is rejected for disclosing the same subject matter as claim 5.

64. Claims 40 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baker as applied to claims 1 and 2, Davis as applied to claim 4, and Harn as applied to claim 8.

65. As per claim 40, Baker discloses a method for controlling access to data held on a computer system as requestable web pages (claim 1), the method including:

Allocating computer system users between a plurality of user groups as members thereof,

Labeling user groups with respective data access levels associated with member groupings (claim 1),

Using a proxy server to:

Receive a request for a web page from a client computer system having web browser software and client proxy software and controlled by a requesting member of a user group, and

Art Unit: 2132

Give access to a requested web page to the requesting member if it is a member of a user group labeled with a data access level in which the hierarchy is equal to or above the data access level of the requested web page (claim 2).

Baker does not disclose:

Labeling the web pages with meta tags defining a hierarchy of data access levels for an access control list.

However, in view of claim 6, the examiner applies the same argument in deducing obviousness for one to apply meta tags with the security access level comprised therein to the datasets in Barker (see claim 6).

Baker does not disclose wherein each member has a key for signing data and a certificate indicating groupings to which that member belongs and wherein the proxy server:

sends data for signature to the client computer system and obtain the requesting member's certificate,

receives data from the client computer system,

verifies that the received data is:

signed with the requesting member's key,

a signed equivalent of the data sent to the requesting member for signature, and

signed with a key from a certificate which is not time expired or invalid, and

if the received data is verifies as aforesaid, check the data access level of the requesting member's user group against the access control list.

Harn and Davis combined do teach these limitation, wherein as applied in claim 4, Davis teaches the use of user certificates for gaining access and recognizing users in a multi-level security protocol and Harn as applied in claim 8, discusses the well known method of challenge response user authentication. The rejections to claims 4 and 8 are applied herein, and one of ordinary skill in the art would be able to see the motivation and obviousness of combining these methods with Baker, as Harn and Davis discuss common features in database access and access control systems. Motivation, as would easily be deduced by one of ordinary skill, is to increase the security and authentication stages by requiring user certificates and private keys for challenge response identification.

66. Claim 43 is rejected because it discloses the same subject matter as claim 40.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

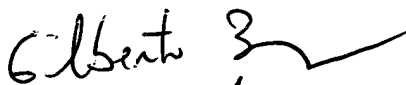
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau  
Examiner  
Art Unit 2132

BB  
\*\*\*

  
GILBERTO BARRON JR  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100